

Authentication with Social Networks

Specification:	OAuth Authentication With Social Networks
Description:	Ability to Sign in with LinkedIn, Google+, Facebook
Target	PLF 4.3
Owner	Patrice Lamarque
Status	DRAFT - REVIEW - VALIDATED

Table of Contents

- [Rationale](#)
- [Functional Specification](#)
 - [Login Screens](#)
 - [Sign In Flow](#)
 - [Register Form](#)
 - [User Account Settings](#)
 - [User Administration](#)
- [Technical Requirements](#)
 - [Providers](#)
 - [Username Generation](#)
 - [Buttons](#)
 - [Upgrades](#)
- [References](#)

Rationale

With the dominance of social networks like Facebook, Google+ or LinkedIn as the ubiquitous identification and authentication method of internet users, it has become a high expectation for a public-facing website to provide authentication through them. While employee facing scenario may not use it, external facing sites built with eXo Platform need to provide a facility to connect to these major social networks. [oAuth 2](#) has imposed as the de facto standard adopted by major social network players, so it should be supported by Platform as an authentication method.

GateIn has implemented such feature as of [version 3.6](#). Also, the eXo Community website has done a PoC implementation to review the use case on a public facing scenario. It is necessary that the implementation provided by this specification provides a continuity to replace seamlessly the PoC implementation by the official one.

Functional Specification

Login Screens

The login screens in eXo Platform need to be updated in order to add buttons for signing in with social networks.

Version	ID	Description
4.3	LOGIN_01	<p>By default, the Login dialog (accessible from /portal/acme > Login) should provide 4 sign up buttons : Facebook, Google, LinkedIn, Twitter</p> <p>there is a highlighting effect on mouse over buttons (see BD-1941)</p>
4.3	LOGIN_02	<p>By default, the Login page (accessible from /portal/login) should provide 4 sign up buttons : Facebook, Google, LinkedIn, Twitter</p> <p>there is a highlighting effect on mouse over buttons (see BD-1941)</p>




4.3	LOGIN_03	The list of buttons should be dynamically bound to the list of active providers (see technical guidelines)
4.3	LOGIN_04	Users with an established link to a social network (see below how to do this) AND a password in eXo, should be able to log in either via <code>with in With...</code> button, or via the eXo Platform's username/password form.
4.3	LOGIN_05	<code>Remember Me</code> feature should work seamlessly when authentication has been done via a social network button

Sign In Flow

The Sign in flow relies on oAuth, but can handle the creation of an user account.



Version	ID	Description
4.3	FLOW_01	<p>When clicking "Sign in With" an oAuth authentication flow starts with the social network. The user may be redirected to the social network if :</p> <ul style="list-style-type: none"> • he has not authorized eXo to access his user data in the social network • he is not currently logged in the social network <p>✅ Each social network has its own way to manage authentication at this stage. For instance, if the user is not already logged in, LinkedIn appends a login/password form on the page.</p>


		<p>authorization page, while Google redirects to a dedicated login/pwd form before coming back to the authorization page.</p>
4.3	FLOW_01b	<p>if user did not accept on the oauth authorization page, he should be redirected back to the eXo page where on the Sign in With... button.</p>
4.3	FLOW_02	<p>After user has granted authorization, if the social network account is already linked to an eXo user account (<i>oauth-username</i> link in the chart), the user is authenticated and redirected to eXo.</p> <p>  The user should be redirected back to the page he tried to access initially. If he went directly to login the portal resolves the page to display as usual </p>
4.3	FLOW_03	<p>The providers should extract the following user profile attributes from the social network and use them to initialize eXo Platform user account : Username, First Name, Last Name, Email, Avatar picture.</p> <p>  These informations can be accessed from the user profile page (menu <i>User</i> > <i>My Profile</i>) The same informations (except the avatar) are also available in user account settings popup (menu <i>User</i> > <i>Settings</i>) </p>
4.3	FLOW_04	<p>If the provider is configured accordingly (see REG_03), the registration form is displayed and the Sign in flow terminates with REG_02. Otherwise, an attempt to create an account automatically on the fly is made.</p>
4.3	FLOW_05	<p>eXo attempts to detect if a user account already exists for this social network user by the following means :</p> <ul style="list-style-type: none"> • the username extracted from the social network matches an existing eXo user name • the email address extracted from the social network matches an existing user account email • current browser has logged on this eXo server within less than 1 hour (user name detected via cookie)
4.3	FLOW_06	<p>if an existing user account is detected a dialog invites the user to use the detected account.</p> <ul style="list-style-type: none"> • Title : <i>Existing Account Detected</i> • Message : <i>We have detected that an eXo account already exists for \$DETECTED. If you would please enter your eXo password to confirm</i> where \$DETECTED is either the email or user name detected. • eXo Password a password field • Actions : Confirm, Register New Account
4.3	FLOW_06a	<p>When clicking on Register New Account, the Register popup is displayed pre-filled to let him adjust settings he would like to use.</p>
4.3	FLOW_06b	<p>When clicking on Confirm, an authentication is performed on eXo. If successful, the user is authenticated. an error message is displayed <i>Authentication failed</i>.</p> <p>  Authentication should fail with the message above when the user is disabled (see Disable User Specification) or when password is not set. </p>
4.3	FLOW_07	<p>Once a sign In flow has been done successfully, a link is established between the eXo Platform user account and the social network account. As long as the accounts remain linked, any successful Sign in with that social network account will authenticate in eXo with the linked user account.</p>

		<u>Example</u> : Facebook user account jsmith@example.org was linked with eXo user account jsmith. When with Facebook with jsmith@example.org, I will be automatically authenticated in eXo with the jsmith user account.
4.3	FLOW_08	The <i>Existing Account Detected</i> popup should display a Help icon next to the password field. The tooltip is : <i>initially registered with a social account, please sign in with this account to update your user settings and link social accounts.</i>

Register Form


A Register form is displayed in a popup when the provider is configured to use it or when user explicitly requests to create a new account.

Example of the register popup on top of login (/portal/login) screen

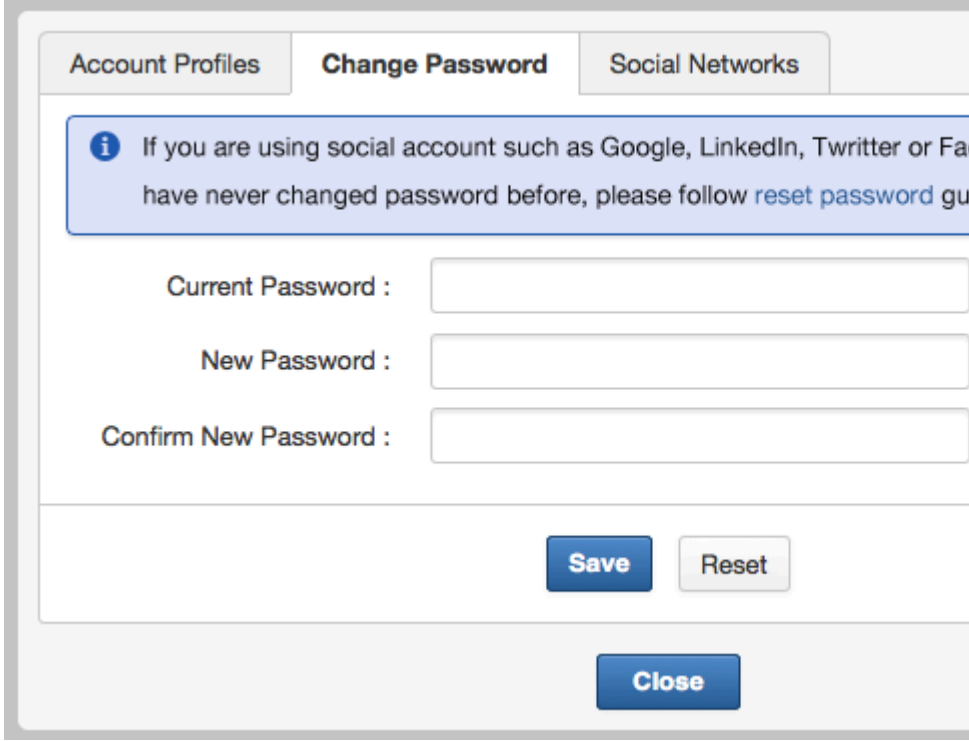
Version	ID	Description
4.3	REG_00	the Register Form is a popup displayed on the current page. The form has same fields and behaviour as the New Account Form (/acme/newAccount) <i>Example of register popup on acme home</i>
4.3	REG_01	When the Register Form popup appears, it is pre-filled with information extracted from the social network (see FLOW_03).
4.3	REG_02	After the form is submitted successfully, the account is created, the user is authenticated and redirected to the eXo page he initially requested.
4.3	REG_03	An administrator may configure any provider to use the Register Form instead of the on the fly registration (see FLOW_04).
4.3	REG_04	By default, only Twitter provider is configured to display the Register Form. Other providers should be configured to register on the fly.  The documentation should explain that the twitter provider is configured this way because Twitter does not allow retrieving email address which is an important info for any eXo Platform account. For instance, without, user won't be able to reset his password or receive notifications.

User Account Settings

Users can link/unlink their eXo account to social networks via the Account Settings


 For a given provider, only one social network account can be linked.

Version	ID	Priority	Description
4.3	SETTINGS_01	P1	a new "Social Networks" tab is added In User account settings dialog (accessible from User account settings)
4.3	SETTINGS_02	P1	in this tab, for each active provider, a row form is presented : <ul style="list-style-type: none"> \$NETWORK User Name label, where \$NETWORK is the name of the social network (e.g. Facebook, Google+, LinkedIn) a text field for the user name in the social network

			<ul style="list-style-type: none"> a Link button with <i>Link social account</i> label or an Unlink button with <i>Unlink s</i> below)
4.3	SETTINGS_03	P1	The text field is readonly. It has a value when the eXo user account is linked with a social r empty.
4.3	SETTINGS_04	P1	A Social network username can only be associated with a single eXo user account at a tim with an user name that is already linked to another account, an error message is displayed <i>already linked to an eXo user name. Please enter another one or ask an administrator to ur</i>
4.3	SETTINGS_05	P1	When clicks on the Unlink button, the link between the social network and the eXo Platfo field is reset to blank. Hence, this user name can be used to link another eXo account or is explained in FLOW_01.
4.3	SETTINGS_06	P2	<p>Users who just registered on the fly via a Sign in with button will not have a password They should be able to set a password via their Account Settings, reset it via Forgot should be able to set it for them via Community Management portlet.</p> <p>Once the password is set, the users can either log in via login/password or via the social ne</p>
4.3	SETTINGS_06.01	P2	<p>There is reset password guidelines link to request users to follow if they want to change the Change Password</p> <p>If you are using social account such as Google, LinkedIn, Twitter and have never changed password before, please follow reset passwor</p> 
4.3	SETTINGS_06.02	P2	<p>When reset password link is clicked:</p> <ul style="list-style-type: none"> An information message is displayed: Reset password guidelines has Please check your email ! Forgot Password function is executed, users receive an email to guide their password.

User Administration

Administrators can link/unlink user accounts to social networks via the community management portlet.

 For a given provider, only one account can be linked.

Version	ID	Description
4.3	ADMIN_01	In <code>User Profile</code> tab of community management (accessible from Administration > Groups and Roles > User Management > Edit User Info), a <code>Social Networks</code> tab is added in Personal Info
4.3	ADMIN_02	in this tab, the same forms as described in SETTINGS_02 are displayed.
4.3	ADMIN_03	On <code>Save</code> , if the social network user name field was cleared, the current eXo account is unlinked to the new social network user name .
4.3	ADMIN_04	On <code>Save</code> , if the social network user name field was changed, then it should be unlinked to previous social network user name and linked to the a new (changed) social network user name. If the field was left blank, it should only be unlinked.

Technical Requirements

This section provides requirements that may not be functionally testable rules via un UI, but may impact implementation.

Providers

ID	Description	
4.3	PROVIDERS_01	3rd party developers should be able to provide the implementation of another oAuth provider (e.g GitHub).
4.3	PROVIDERS_02	providers should be pluggable via an extension
4.3	PROVIDERS_03	an administrator should be able to disable and configure providers via <code>exo.properties</code>

Username Generation

Version	ID	Description
4.3	USR_01	The username generated in eXo Platform should be a specific for each authentication Provider
4.3	USR_01a	Username may be extracted from an email address. In that case, only the leading part (before the @) is used. Example : <code>john.smith@example.com</code> would extract to <code>john.smith</code>
4.3	USR_02	For Facebook provider, eXo username should be extracted (see USR_01a) from the primary email address as shown in General Account Settings on facebook.com
4.3	USR_03	For LinkedIn provider, eXo username should be extracted (see USR_01a) from the primary email address as shown in Account and Settings on linkedin.com :
4.3	USR_04	For Twitter provider, eXo username should use the twitter @handle such as shown in the My Profile on twitter.com :
		For Google+ provider, eXo username should be extracted (see USR_01a) from the primary email address

4.3	USR_05	such as shown in the My Account on google.com :
-----	--------	---

Buttons

Version	ID	Description
4.3	BTN_01	Sign in with... buttons should be easy to customize. Here are two examples of custom login form that should be possible to implement with css :

Upgrades

Version	ID	Description
4.3	UPG_01	Upgrading from a previous version of eXo Platform, should not enable the oauth providers automatically.

References

- [Gatein Feature](#)
- [oAuth](#)